REMARKS

Upon entry of this amendment, claims 1-3, 5-7, 9-11, 13-16 and 18-23 are all the claims pending in the application. Claims 20-23 have been added as new claims, and claims 4, 8, 12 and 17 have been canceled by this amendment. No new matter has been added.

I. Claim Rejections under 35 U.S.C. § 103(a)

Claims 1-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Goss (U.S. 4,956,863).

Claim 1, as amended, recites that the random number generator and the public key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the public key generator, wherein the random number generator generates a new random number after the calculation of the public key ya is completed so that the public key ya becomes a function of the random number, and wherein the arithmetic algorithm of the public key generator is not revealed outside of the one semiconductor integrated circuit. Applicant respectfully submits that Goss does not disclose, suggest or otherwise render obvious at least the above-noted combination of features recited in amended claim 1.

Regarding Goss, Applicant notes that this reference relates to a public key exchange cryptographic system, in which two user devices establish a common session key by exchanging information over an insecure communication channel, and in which each user can authenticate the identity of the other (see Abstract). With respect to the communication channel in Goss, Applicant notes that Goss discloses the possibility of adding a signature to a key in the case that the communication channel 26 is being eavesdropped (see Fig. 3).

Applicant notes, however, that Goss does not disclose the ability to prevent the eavesdropping of certain values, algorithms and variables, such as a value of Xa', a value of "signed Ya", an algorithm performed by key generator 18, a digital signature algorithm, and variables α and p.

In this regard, Applicant notes that the above-noted values, algorithms, and variables are elements that constitute a basis of a public key cryptosystem, and when such elements are attacked and information is leaked, the information on the communication channel 26 of Goss may be easily stolen. To this end, Applicant notes that in Fig. 5 of Goss, which depicts the cryptographic processor 60, it would be easy to observe the contents of RAM 68, ROM 70, data bus 64, and address bus 66, and thus, the above-noted algorithms could be easily stolen.

As noted above, claim 1 has been amended to recite that the random number generator and the public key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the public key generator, wherein the random number generator generates a new random number after the calculation of the public key ya is completed so that the public key ya becomes a function of the random number, and wherein the arithmetic algorithm of the public key generator is not revealed outside of the one semiconductor integrated circuit.

Applicant respectfully submits that Goss does not disclose, suggest or otherwise render obvious the above-noted features recited in amended claim 1. In particular, Applicant notes that because it is possible to perform eavesdropping in the exchange system of Goss so as to uncover certain values, algorithms and variables, such as a value of Xa', a value of "signed Ya", an algorithm performed by key generator 18, a digital signature algorithm, and variables α and p, as discussed above, that Goss clearly does not disclose, suggest or otherwise render obvious the above-noted features recited in amended claim 1.

In this regard, in contrast to the system of Goss, in which eavesdropping is possible, Applicant notes that by providing the above-noted features recited in amended claim 1, it is possible to prevent such eavesdropping.

In view of the foregoing, Applicant respectfully submits that Goss does not disclose, suggest or otherwise render obvious the above-noted combination of features of a random number generator and a public key generator that are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the public key generator, wherein the random number generator generates a new random number after the calculation of the public key ya is completed so that the public key ya becomes a function of the random number, and wherein the arithmetic algorithm of the public key generator is not revealed outside of the one semiconductor integrated circuit, as recited in amended claim 1. Accordingly, Applicant submits that claim 1 is patentable over Goss, an indication of which is kindly requested. Claims 3 and 4, as well as new claim 20, depend from claim 1 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 5, Applicant notes that this claim has been amended so as to recite that the random number generator and the shared key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the shared key generator, wherein the random number generator generates a new random number after the calculation of the public key ya is completed so that the shared key Ka becomes a function of the random number, and wherein the arithmetic algorithm of the shared key generator is not revealed outside of the one semiconductor integrated circuit.

For at least similar reasons as discussed above with respect to claim 1, Applicant respectfully submits that Goss does not disclose, suggest or otherwise render obvious the above-noted features recited in amended claim 5. Accordingly, Applicant submits that claim 5 is patentable over Goss, an indication of which is kindly requested. Claims 6 and 7, as well as new claim 21, depend from claim 5 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 9, Applicant notes that this claim has been amended so as to recite that the random number generator, the public key generator, and the shared key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of arithmetic algorithms of the public key generator and the shared key generator, wherein the random number generator generates a new random number after the calculation of the public key ya and the calculation of the shared key Ka are both completed so that the public key ya and the shared key Ka become functions of the random number, and wherein the arithmetic algorithms of the public key generator and the shared key generator are not revealed outside of the one semiconductor integrated circuit.

For at least similar reasons as discussed above with respect to claim 1, Applicant respectfully submits that Goss does not disclose, suggest or otherwise render obvious the above-noted features recited in amended claim 9. Accordingly, Applicant submits that claim 9 is patentable over Goss, an indication of which is kindly requested. Claims 10, 11 and 18, as well as new claim 22, depend from claim 9 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 13, Applicant notes that this claim has been amended so as to recite that the random number generator, the secret key holding unit, said public key generator, and the shared key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of arithmetic algorithms of the public key generator and the shared key generator, wherein the random number generator generates a new random number after the calculation of the shared key Ka is completed so that the public key ya and the shared key Ka become functions of the random number, and wherein the arithmetic algorithms of the public key generator and the shared key generator are not revealed outside of the one semiconductor integrated circuit.

For at least similar reasons as discussed above with respect to claim 1, Applicant respectfully submits that Goss does not disclose, suggest or otherwise render obvious the above-noted features recited in amended claim 13. Accordingly, Applicant submits that claim 13 is patentable over Goss, an indication of which is kindly requested. Claims 14-16, as well as new claim 23, depend from claim 13 and are therefore considered patentable at least by virtue of their dependency.

II. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Ryogo YANAGISAWA

By: /Kenneth W. Fields/
2008.07.15 18:21:31 -04'00'

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicant

KWF/krg
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 15, 2008